

APPLICATION FOR UNITED STATES PATENT

**METHODS AND SYSTEMS FOR TRANSACTION RECORD DELIVERY USING
THRESHOLDS AND MULTI-STAGE PROTOCOL**

By Inventors:

Marc E. Strohwig
575 Glasgow Circle
Danville, California 94526
A Citizen of the United States

John M. McGinty
421 Maar Avenue
Fremont, California 94536
A Citizen of the United States

W. Olin Sibert
30 Ingleside Road
Lexington, Massachusetts 02420
A Citizen of the United States

Assignee: InterTrust Technologies Corporation
4750 Patrick Henry Drive
Santa Clara, California 95054

Status: Large Entity

007E/0"4T62960

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8800

METHODS AND SYSTEMS FOR TRANSACTION RECORD DELIVERY USING THRESHOLDS AND MULTI-STAGE PROTOCOL

RELATED APPLICATIONS

5 This application claims priority from U.S. Provisional Patent Application Serial No. 60/146,593, entitled "Method and System for Transaction Record Delivery Using Thresholds and Multi-Stage Protocol," filed July 30, 1999, which is hereby incorporated by reference.

COPYRIGHT AUTHORIZATION

10 A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

FIELD OF THE INVENTION

15 The present invention relates generally to systems and methods for electronic communication. More specifically, the present invention relates to systems and methods for managing communications between computer systems involved in a transaction.

BACKGROUND OF THE INVENTION

20 Recent advances in computing and networking technology have enabled a variety of new types of commercial transactions between physically remote parties. For example, many vendors operate Internet web sites at which consumers can purchase the vendor's goods using a credit card or other form of payment. The goods are shipped to the consumer after the payment is received. One class of transactions that is growing in importance involves the sale of digital goods, such as digitally-recorded songs, movies, images, books, reports, and the like. The nature

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6800

of digital goods allows them to be transported over a computer network with relative ease, and/or stored on readily-available and inexpensive storage media, such as diskettes, compact discs (CDs), and the like. Thus, transactions involving digital goods are able to occur virtually instantaneously, as digital goods can be transmitted over the network from the vendor's computer system to the purchaser's computer system in little time.

In other types of transactions, a copy of a digital work might already reside on the consumer's computer system at the time the consumer wishes to purchase it. For example, the consumer may have obtained a copy from a friend, downloaded a copy from the Internet, or obtained a copy by some other means. The content may be encrypted or otherwise packaged so that it cannot be accessed without payment, and the consumer may thus need to contact the content owner or the owner's agent in order to gain access. For example, the consumer may provide the content owner with a credit card payment in exchange for a cryptographic key or other means of unpackaging the content.

There is also an increasing demand for even more flexible business arrangements. For example, a content vendor may wish to allow consumers to purchase content on a pay-per-use basis, and/or may wish to allow consumers to pay for content in a non-traditional manner – such as by allowing the vendor to collect information regarding the consumer's content-usage habits. To facilitate arrangements such as these, a content vendor may provide the consumer with a special rights-management application program that runs on the consumer's computer system and enforces the terms of the consumer's contract with the vendor.

A problem that arises in distributed electronic transactions such as those described above is that of managing the risk borne by content creators and distributors when their content is used by, or distributed to, consumers. For example, content owners will typically wish to prevent consumers from stealing their content and distributing it to others, and will also wish to prevent consumers from circumventing the technical mechanisms by which transactions are conducted and enforced. However, it is desirable to manage this risk in a manner that does not unduly compromise the consumer's content-usage experience, as the more difficult it is for a consumer to access and use electronic content, the less likely it is that the consumer will use it, and thus

00629144-073100
DATE 10-14-96

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

transactions performed by the consumer on the consumer's local system. Upon the occurrence of predefined conditions, transactional records are sent to a remote vendor or clearinghouse. The vendor or clearinghouse can manage the risk it bears by setting the predefined conditions appropriately.

5 In another embodiment, a synchronization protocol for peer-to-peer transactions is disclosed. A local computer system with a storage medium and a communications port is provided, as is a remote computer system with a storage medium and a communications port. The local system's storage medium contains a conditionally-accessible file, and the remote system is communicatively coupled to a database containing authorization records pertaining to
10 the access of the conditionally-accessible file. The local computer system is configured to communicate with the remote computer system to obtain authorization to access the content of the conditionally-accessible file. The synchronization protocol is operable to enable the maintenance of a substantially real-time synchronized copy of the transactional state of the communication between the local computer system and the remote computer system. In one
15 embodiment, the remote system is operable to obtain payment upon receipt of authorization from the database containing authorization records, and upon receipt of an acknowledgment from the local computer system that a user of the local computer system was able to successfully access the conditionally-accessible file.

20 In yet another embodiment, a method for conducting peer-to-peer transactions is disclosed. A request is received by a remote system to give authorization to a user of a local computer system to access data stored on the user's local system. The remote system verifies that the user is authorized to access the data and has sufficient funds in his or her account to pay for this access. The remote system sends authorization to the local computer system to allow the user to access the data. The local computer system is operable to receive the authorization, to
25 give the user access to the data, and to send an acknowledgment to the remote system that the user was given access to the data. The remote system is operable to receive the acknowledgment, remove funds from the user's account, and send a signal to the local system indicating that the transaction is complete. If the local system does not receive this signal within a predefined amount of time after sending the acknowledgment, the local system is operable to

00629114-03100
007E20-4T62960

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

send a second acknowledgment to the remote system. In one embodiment, a user of the remote system is able to set the predefined amount of time that the local computer system waits before sending the second acknowledgment. In yet another embodiment, the remote system is further operable to re-send the authorization to the local computer system if the remote system does not, within a predefined amount of time, receive an acknowledgment from the local system that the local system has given the user access to the content.

In another embodiment, a method is described for delivering transaction records to one or more clearinghouses using intermittent communication and polled acknowledgments, with delivery requirements specified by provider parties. Providers define their tolerance for an acceptable level of risk associated with unprocessed records by specifying thresholds. These thresholds are capable of acting in concert and of specifying age, record count, financial value, average age, age-weighted value, and other predefined characteristics. Records are delivered whenever communication is convenient, and acknowledgments are polled or repolled on the same basis. Records may go through multiple stages of processing – e.g., receipt, payment initiation, successful payment – at one or more destination systems, each of which stages returns an acknowledgment, and each of which stages may be governed by different thresholds.

In yet another embodiment, a method of granting access to a piece of content is disclosed. In accordance with this embodiment, a first computer system sends a request to a second computer, the request seeking permission to access the content. The first computer system also initiates the execution of a monitoring process. The monitoring process is able to detect acknowledgments from the second computer system. The second computer system receives the request from the first computer system and determines whether it should grant or deny the request. If the second computer system decides to grant the request, it sends a status signal to the first computer system. Upon receipt of the status signal, the first computer system releases the content for use, and sends a first acknowledgment to the second computer system. The monitoring process is operable to resend the first acknowledgment to the second computer system if the first computer system fails to receive a response to the first acknowledgment within a predefined amount of time.

00629144-073100
DOT 2.0 "4T62960

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6800

5

In another embodiment, a method for managing the transmission of transactional audit records from a first computer system to a clearinghouse is disclosed. In accordance with this embodiment, a first count is maintained at the first computer system of the number of audit records accumulated at the first computer system. If the first count exceeds a predefined amount, then the audit records are scheduled for delivery to the clearinghouse. When the audit records are delivered to the clearinghouse, the clearinghouse may send an acknowledgment to the first computer system, the acknowledgment identifying the number of audit records that the clearinghouse has processed. Upon receipt of this acknowledgment, the first computer system decrements the first count by an amount equal to the number of audit records identified in the acknowledgment from the clearinghouse. In one embodiment, the first computer system also maintains a second count, the second count keeping track of the total value of the unpaid receipts from transactions conducted on the first computer system. When the audit records that correspond to these transactions are processed by the clearinghouse, the clearinghouse sends back an acknowledgment to the first computer system indicating that these receipts have been paid. The first computer system then decrements the second count accordingly.

10

15

These and other features and advantages of the present invention will be presented in more detail in the following detailed description and the accompanying figures which illustrate by way of example the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

20

The present invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

Fig. 1 illustrates a system for conducting transactions in accordance with the principles of the present invention.

25

Figs. 2 shows a computer system for practicing embodiments of the present invention.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

Figs. 3A, 3B, 3C, 3D, 3E, 3F, and 3G illustrate various aspects of a communications protocol in accordance with an embodiment of the present invention.

Fig. 4 illustrates the structure and function of a threshold object in accordance with an embodiment of the present invention.

Fig. 5 illustrates the use of thresholds in accordance with an embodiment of the present invention.

Figs. 6A, 6B, and 6C illustrate the form of several types of conditional expressions that can be used with thresholds in accordance with embodiments of the present invention.

Fig. 7 illustrates the flow of audit records and acknowledgments between a clearinghouse and a consumer's system.

Fig. 8 illustrates the use of thresholds in an electronic transaction in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

A detailed description of the invention is provided below. While the invention is described in conjunction with several embodiments, it should be understood that the invention is not limited to any one embodiment. On the contrary, the scope of the invention is limited only by the appended claims and encompasses numerous alternatives, modifications, and equivalents. For example, while embodiments are described in the context of systems and methods for communicating between physically remote computer systems via a network, those skilled in the art will recognize that the disclosed systems and methods are readily adaptable for broader application. For example, without limitation, the systems and methods of the present invention could also be readily applied in the context of inter-component communications in an integrated computer system. In addition, while numerous specific details are set forth in the following description in order to provide a thorough understanding of the present invention, the present invention may be practiced according to the claims without some or all of these details. Finally,

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.

STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8800

program 110 such as an electronic jukebox, application 112 processes the consumer's request, charges the consumer's account, makes a record of the transaction, decrypts the content, and releases it to rendering application 110. Application 112 may also transmit records that relate to the transaction 122 to one or more clearinghouses 106 whose responsibility it is to ensure that the vendor is paid and the consumer is charged appropriately. Records 122 may, for example, contain information regarding the consumer's use of the content, such as the amount the consumer should be billed, or information that the consumer has agreed to provide regarding his or her usage habits. Clearinghouses 106 and/or vendors 102 may also communicate with a financial authorization center, such as bank 114, in order to obtain information regarding the consumer's credit balance and to charge the consumer's account. As described in more detail below, the present invention provides systems and methods for managing such transactions in an efficient, flexible, and secure manner.

In one embodiment, transaction processing software 112 comprises an instance of the InterRights Point™ software produced by InterTrust Technologies Corporation, of 4750 Patrick Henry Drive, Santa Clara, California 95054. In this embodiment, content 118 and/or audit records 122 may be packaged in DigiBox® secure containers, also developed by InterTrust. However, it will be appreciated that for purposes of practicing the present invention, any content container or file format and/or transaction processing application can be used. Moreover, it should be understood that while in one preferred embodiment communications between consumers 104, vendors 102, and/or clearinghouses 106 are encrypted, digitally signed, packaged in secure containers, or otherwise protected, such protection is not required.

Thus, it should be appreciated that Fig. 1 is provided for purposes of facilitating a discussion of the present invention, and that a variety of modifications can be made to the basic architecture shown therein. For example, in some embodiments vendors 102 may collect transactional data 122 directly from consumers 104, and thus may obviate the need for separate clearinghouses 106. As another example, while Fig. 1 shows vendors 102 and clearinghouses 106 communicating with consumers 104 via a network 108 such as the Internet, it should be appreciated that any suitable form of communication could be used. For example, consumer's system 104 might comprise a handheld electronic appliance, such as a portable digital assistant, a

handheld digital media player, or the like, and clearinghouse 106 might comprise a relatively-secure computer system at the consumer's site (e.g. a personal computer with a special chip or smart-card attachment) – possibly connected to a remote server via a dedicated connection (e.g., DSL or ordinary dial-up). In such an embodiment, consumer's system 104 might use the systems and methods of the present invention to communicate with the clearinghouse's local system 106 via an infrared or radio-wave signal, or by simply connecting a cable from the consumer's system to the clearinghouse's local system. The clearinghouse's local system might then communicate with the clearinghouse's remote system using the systems and methods of the present invention and/or by using well-known means for secure communication (e.g., SSL).

Fig. 2 provides a more detailed illustration of the structure and operation of consumer's system 104 in accordance with an embodiment of the present invention. As noted above, system 104 may consist of any suitable device, including without limitation a personal computer, a portable audio or video player, a television set-top box, a telephone, a personal digital assistant, or the like. As shown in Fig. 2, system 104 will typically include:

- a processing unit 216;
- system memory 218, preferably including both high speed random access memory (RAM) and read-only non-volatile memory (ROM) for storing programs and data for use and execution by processing unit 216;
- a bulk non-volatile storage unit 270, comprising erasable non-volatile memory, such as a magnetic, fixed disk (e.g., a hard disk) and/or flash memory, for storing protected content files, application programs, data, and the like;
- one or more input/output devices, such as:
 - network interface 210 for communicating with other systems via a network 108 such as the Internet;
 - I/O port 212 for connecting to one or more peripheral devices; and/or

- one or more disk drives 214 for reading from, and/or writing to, diskettes, compact discs, DVDs, and/or other computer-readable media;
- a user interface 226, including a display 228 and one or more input devices, such as keyboard 206 and mouse 208; and
- one or more internal buses 240 for interconnecting the aforementioned elements of the system.

The operation of system 104 is controlled primarily by programs contained in system memory 218 and executed by the system's processing unit 216. For example, system 104 might contain one or more rendering applications 110 that are operable to display or otherwise present content to the user. In the case of protected content 118, in one embodiment rendering applications 110 submit requests to access the content to transaction processing application program 112. Transaction processing application 112 then grants or denies the request using the techniques described elsewhere herein.

Programming code for performing the electronic transaction methods described herein is preferably incorporated into transaction processing application 112 (e.g., directly or by linking a library module). While the methods of the present invention protect against certain forms of attack and/or circumvention – such as disconnecting the consumer's system 104 from network 108 during certain critical points of a transaction – these methods also derive some of their security from the integrity of transaction processing application 112 itself. Accordingly, preferred embodiments of the present invention make use of hardware and/or software security techniques to ensure that transaction processing application 112 operates as intended.

For example, in one embodiment system 104 may include a special-purpose protected processing environment 288, such as that provided by an integrated circuit housed in a tamper-resistant hardware package. As shown in Fig. 2, protected processing environment 288 may include non-volatile memory 289, volatile memory 290, a processor 291, a tamper-resistant barrier 293, and a communications port 294 for communicating with other components of system 104. Use of a protected processing environment is advantageous, in that it provides an area that

is shielded from unauthorized observation or modification in which to run sensitive programs and to store cryptographic keys and other information. For example, transaction processing application 112, or selected portions thereof, can be loaded into RAM 290 of protected processing environment 288 and executed by CPU 291, thus protecting the operation of transaction processing application 112 from being tampered with or otherwise modified. Additional information about implementations of a protected processing environment can be found in commonly-assigned U.S. Patent No. 5,892,900, "Systems and Methods for Secure Transaction Management and Electronic Rights Protection," issued April 6, 1999 ("the '900 patent"), and commonly-assigned U.S. Provisional Application No. 60/150,126, "Secure Processing Unit Systems and Methods," filed August 20, 1999, each of which is hereby incorporated by reference in its entirety.

In another, somewhat less-secure embodiment, transaction processing application 112 makes use of software obfuscation and other software self-defensive techniques to protect itself from undetected tampering. Additional information on suitable software obfuscation and self-defensive techniques can be found in the '900 patent, and in commonly-assigned U.S. Patent Application No. 09/095,346, entitled "Obfuscation Techniques for Enhancing Software Security," filed June 9, 1998, and commonly-assigned U.S. Patent Application No. _____, entitled "Software Self-Defense Systems and Methods," filed July 31, 2000, each of which is hereby incorporated by reference in its entirety.

In addition, system 104 might advantageously include hardware and/or software for providing secure bulk storage for sensitive bookkeeping, usage, or other information. For example, a specialized hardware database can be used, and/or relatively-secure software storage protection mechanisms (or hybrid software-and-hardware mechanisms), such as those set forth in the '900 patent and in commonly-assigned U.S. Patent Application No. _____, entitled "Trusted Storage Systems and Methods," Maheshwari et al., filed July 17, 2000 ("the Maheshwari application"), which is hereby incorporated by reference in its entirety.

While Fig. 2 sets forth the general architecture of a typical consumer system 104, it will be appreciated that a number of modifications could be made to the basic structure shown therein

09629114-073100
001E20-HT6296

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6800

without departing from the principles of the present invention. Moreover, it will be appreciated that clearinghouses 106 and vendors 102 may make use of similar or identical systems.

Immediate Transaction Protocol

In an "immediate transaction," a consumer pays for electronic or other content at the time the content is released to the consumer. For purposes of illustration, an exemplary technique for conducting such a transaction is described in the context of a transaction between consumer 104 and clearinghouse 106, although it will be appreciated that such a transaction could just as easily be conducted between any suitable set of parties, including without limitation consumer 104 and vendor 102, vendor 102 and clearinghouse 106, and so forth.

When conducting an immediate transaction, it is important to maintain synchronization between the state of the consumer's system 104 and the state of the clearinghouse 106. For example, it would be undesirable for records on the consumer's system 104 to indicate that the consumer had purchased a piece of content, while records at the clearinghouse 106 indicated that the consumer had not. Nor would it be desirable for records at the clearinghouse 106 to indicate that the content had not been released to the consumer, when, in fact, it had been released.

However, maintaining synchronization between peers in an electronic peer-to-peer communication – such as the communication between consumer 104 and clearinghouse 106 – is a difficult task. For example, if the consumer's system sends a signal to the clearinghouse, there is generally no way for the consumer's system to know whether the clearinghouse received the signal, save for receiving an acknowledgment from the clearinghouse indicating that the signal was received. However, the clearinghouse will similarly not know if the consumer's system received that acknowledgment, unless the consumer's system, upon receipt of the acknowledgment, sends its own acknowledgment back to the clearinghouse. This second acknowledgment will necessitate a third acknowledgment, and so forth, thus presenting the system designer with a potentially infinite recursion.

One way to break the recursion is to have both the consumer and the clearinghouse send their acknowledgments to a third party, who then sends a signal back to each of the parties

096914-03100
NOTE: 4-16-96

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L. L. P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

09629114-073100

payment on behalf of the content distributor. However, it should be appreciated that the local computer system and the remote computer system can be those of any suitable entity. Moreover, while for ease of explanation, actions may be described as being initiated or performed by the local system or the remote system, it will be appreciated that these actions are typically carried out by appropriate software, such as transaction processing application 112, or hardware contained within those systems.

As shown in Fig. 3A, a consumer may download or otherwise obtain content that is encrypted or stored in some other manner that renders it practically inaccessible (302). Upon receiving the consumer's request to access the content (304), the consumer's local system 104 generates one or more audit records and places a job 305 (explained in more detail below) into a job queue maintained by application 112 (306). For example, application 112 may include a thread that functions as a manager of background tasks placed in the queue. Job 305 preferably includes an identification of the audit record to which it corresponds and an indication of whether the transaction associated with the audit record has succeeded or failed (e.g., a two state status flag indicating *success* or *failure*). When the job is first placed in the job queue, its flag is initialized to *failure*. Local system 104 then initiates communication with a remote system, such as clearinghouse 106 or vendor 102, to obtain authorization to access the content. In addition, a copy of the audit record 307 is sent to the remote system (308).

As shown in Fig. 3B, the remote system receives audit record 307 and begins processing the transaction to which the audit record corresponds (310). For example, the remote system may contact a bank 114 or other financial authority to determine whether the consumer's credit card is valid and has enough available credit to cover the transaction described by audit record 307. As shown in Fig. 3B, in some embodiments, the remote system may send an optional signal 314 to the local system in order to provide an estimate of the time needed to complete the authorization process (312). Upon receipt of such a signal, the local system may, for example, display a message to the consumer indicating how long the authorization process is expected to take. In addition, the local system may send the remote system a return acknowledgment.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

As shown in Fig. 3D, upon receiving acknowledgment 328 (368), the remote system completes its part of the transaction by, e.g., posting the transaction to the consumer's credit card, withdrawing funds from the consumer's account, and/or taking other appropriate action (332). The remote system also sends an acknowledgment 336 – i.e., the resend-acknowledgment signal – to the local system, indicating that the remote system received the local system's acknowledgment 328 and completed its end of the transaction (334).

As shown in Fig. 3E, upon receipt of resend-acknowledgment signal 336 (338), the local system removes job 305 from its background job queue (339). In some embodiments, the local system may also send a request for session closure (e.g., RSCX) to the remote system (and receive an acknowledgment thereto) before closing the line of communication (340). Fig. 3F summarizes the sequence of communications between the local and remote systems in the embodiment described above.

Due to inefficiencies, failures, or attempts to attack the system – occurring at the local system, at the remote system, and/or on the network – the communication between the local system and the remote system may not proceed in the manner described above. For example, one or more of the signals between the local system and the remote system may be lost, delayed, diverted, or corrupted. The present invention provides mechanisms for efficiently responding to such failures in a manner that is consistent with system rules and security constraints. Examples of several fault conditions, and the system's response thereto, are provided below.

Local System Fails to Receive Status Signal 318. After the local system sends an audit record to the remote system (i.e., block 308 in Fig. 3A), the local system waits for transaction status signal 318 from the remote system (i.e., block 342 in Fig. 3C). If the local system does not receive the status signal (or does not receive it in a predefined amount of time), then in one embodiment the local system resends the audit record (or a message indicating that no status signal has been received), repeating this process a predetermined number of times before giving up and, e.g., informing the consumer that the remote system is not responding or that the network connection has failed. This process can be integrated with the resend job 305 performed by application 112's background manager, or can be performed independently. In other

embodiments, the local system gives up without retrying after a predefined amount of time has elapsed. If the local system does not receive transaction status signal 318, the local system does not release the content to the consumer or otherwise perform the action for which authorization was sought. Moreover, since the local system will thus fail to send acknowledgment 328 to the remote system, the remote system will not debit the consumer's account.

Remote System Fails to Receive Acknowledgment 328. Similarly, after the remote system sends a transaction status signal 318 to the local system, indicating that the transaction has been authorized, the remote system waits for an acknowledgment 328 from the local system indicating that the transaction was successfully completed (i.e., block 368 of Fig. 3D). As described above, upon receipt of acknowledgment 328, the remote system proceeds with completing its end of the transaction by, e.g., capturing the authorized, and possibly locked, funds (i.e., block 332 of Fig. 3D). However, if the remote system does not receive acknowledgment 328, the remote system will not authorize capture of the funds. Moreover, the remote system will not send signal 336 to the local system, which, as described below, will cause the local system to resend signal 328 (if it was sent in the first place).

In addition, if the remote system does not receive the indication 328 from the local system that the transaction has completed (or failed), the operator of the remote system might take appropriate defensive action – e.g., contact the consumer or owner of the local system, put a hold on the consumer's account, check the network and/or the remote system for failures, etc. – thus preventing an attacker from defrauding the system, and thus enabling a rapid diagnosis of equipment problems.

Local System Fails to Receive Acknowledgment 336. If the local system fails to receive resend-acknowledgment signal 336 within a predefined period (e.g., 1, 2, or 5 minutes) after releasing content to the consumer and sending acknowledgment 328 to the remote system (and/or a predefined amount of time after the initiation of resend job 305), then the local system automatically resends the acknowledgment 328 and/or a copy of the audit record 307 indicating that the transaction was successfully completed. As described above, upon receipt of this signal,

09629114-073100
NOTED - ATT 22960

In a preferred embodiment, the operator of the remote system is able to specify the amount of time, x , that the local system's background resend job should wait before resending the acknowledgment 328 (and/or the number, y , of unacknowledged transmissions of acknowledgment 328/377 to tolerate before sending/storing an error or message 381). For example, a specification of this time period 320 can be sent to the local system along with the authorization to release the content 318, or can be provided at another suitable time. Thus, content owners and distributors are provided with a mechanism for controlling the conduct of the transaction and their exposure to system failures.

Local System Releases Content Despite Receiving a Negative Status Signal 318. In a preferred embodiment, the local system automatically sends the remote system a status report when content is released, and/or when an audit record's status is changed from *failure* to *success* (unless the remote system requests that this report not be sent). This communication is preferably integrated with the background communication process 305 that is queued whenever content is requested (or, in some embodiments, released). As described above, the background process 305 remains in operation until a communication is received from the remote system indicating that the remote system was able to complete its side of the transaction. Thus, if the local system fails to obey the remote system's instructions not to release content, the operator of the remote system will be informed and can take immediate defensive action. In order to avoid detection by the remote system, an attacker may thus need to keep the local system disconnected from any communications medium (such as the Internet) by which the background processing job can transmit the message to the remote system. This will typically not be a very attractive option for the attacker, especially if the value of the purchased content is relatively small in relation to the inconvenience of being unable to fully use the local system.

One of ordinary skill in the art will appreciate that for purposes of clarity, a description of certain well-known signals dictated by the underlying network protocol or transport layer (e.g., TCP/IP, HTTP, FTP, AAL 5, etc.) has been omitted from the foregoing discussion. In addition, while the discussion has focused primarily on two-party transactions, it will be appreciated that the present invention is readily adaptable to transactions involving more than two parties. Moreover, while it has been implicitly assumed that the conditionally-accessible content resides

on the consumer's local system during the process described above, it will be appreciated that this content could be stored at a remote location, including on remote system 102 or 106, during all or part of the process without departing from the principles of the present invention.

Moreover, while a communications protocol has been presented in the context of immediate transactions between a consumer 104, vendor 102, and/or clearinghouse 106 involving the purchase of electronic content, it will be appreciated that the protocol can be readily applied to other situations. For example, the protocol could be used to manage the transfer of funds from clearinghouse 106 to vendor 102, to manage the transfer of audit records between consumer 104 and clearinghouse 106 in a non-immediate transaction, and/or to facilitate a variety of other types of transactions or communications.

Deferred Transactions: Thresholds

The foregoing discussion has focused primarily on transactions in which the consumer is expected to pay for content at the time it is released for use (or at effectively the same time). As described above, such transactions generally require a connection between the consumer's system and the vendor's system (or clearinghouse). However, to enhance performance and fault tolerance, and to facilitate a wider range of business relationships between vendor and consumer, it may also be desirable to allow the consumer to purchase and use content without connecting to the vendor's system, deferring payment until a later time when connecting to the vendor's system is more convenient. While deferred transactions provide the consumer with more flexibility, and thus provide the content vendor with increased sales opportunities, deferred transactions also present the vendor with increased risk, as an attacker might take advantage of the relative isolation of the consumer's computer system to attempt to modify or steal protected content, to delete or alter transactional records, or to tamper with the operation of the transaction processing application. The present invention provides systems and methods that enable content owners and vendors to manage their exposure to such attacks.

In a preferred embodiment, secure deferred transactions are enabled by providing the consumer with a transaction processing application 112 that resides on the consumer's system 104 and conducts and manages transactions on the vendor's behalf. When the consumer

purchases a piece of content, application 112 decrypts the content and releases it to the consumer. As shown in Figs. 1 and 5, application 112 also creates one or more audit records 122 detailing, among other things, the price the consumer paid for the content, the identity of the clearinghouse 106 to which the audit records should be sent for processing, and the like. To prevent undetected deletion or modification, application 112 preferably stores audit records in secure, tamper-resistant storage, such as that described in the '900 patent or the Maheshwari application, both of which were previously incorporated by reference. In addition, application 112 preferably incorporates software self-defense techniques and/or is run in a secure environment such as protected processing environment 288 in Fig. 2.

As shown in Fig. 5, in one embodiment audit records 122 may reference one or more clearinghouse information (CHInfo) objects 510 and/or budgets 512, which, in turn, may reference one or more thresholds 514. A CHInfo object 510 is a programming construct that may be associated and/or packaged with protected content 118. A CHInfo object 510 identifies the clearinghouse associated with the content, the forms of payment accepted by the clearinghouse, and a list of thresholds that control the delivery of payment or audit records to the clearinghouse. Similarly, a budget object 512 is a programming construct that is typically provided to (and/or instantiated within) the consumer's transaction processing application 112 by an issuer of credit or a provider of debit accounts or electronic cash. The consumer's budget contains information about the consumer's account (e.g., balance, available credit, etc.) and a list of thresholds governing the payment of accumulated balances and the like.

In general terms, thresholds 514 provide a mechanism for monitoring transactions on the consumer's system and for triggering predefined actions when certain conditions occur. For example, thresholds 514 may place limits on the quantity of offline charges or audit records that the consumer can accumulate before connecting to a clearinghouse, budget provider, or vendor's computer system. Thus, a threshold 514b on budget 512 can be viewed as limiting the exposure of the budget provider, while a threshold 514a on CHInfo object 510 can be viewed as protecting the rights of the clearinghouse.

Fig. 4 provides a more detailed illustration of the structure of a threshold object 514 in accordance with an embodiment of the present invention. As shown in Fig. 4, a threshold 514 typically includes a type definition 412 (e.g., acknowledgment, paid, or controlled), one or more triggers 401, and a variety of state information 406 – such as a current value (e.g., a currency amount), a current count (e.g., a count of accumulated audit records), and a last acknowledgment (e.g., an indication of the last time the consumer's system communicated with a clearinghouse).

One of ordinary skill in the art will appreciate that the structure and functionality depicted in Fig. 4 can be readily-implemented in one or more data structures maintained by transaction processing application 112. For example, in one embodiment thresholds are implemented as objects in an object-oriented programming language such as C++ or Java. However, one of ordinary skill in the art will appreciate that the functional relationships depicted in Fig. 4 can be readily implemented in any suitable fashion without departing from the principles of the present invention.

The variables that comprise a threshold's state may be incremented when a transaction occurs (e.g., when a consumer purchases or uses a piece of content), and may be reset or updated in response to events such as the successful delivery of audit records to a clearinghouse. For example, if a customer buys a piece of content for \$5.00 and generates two audit records in the process, the VALUE variable of the appropriate threshold would be increased by \$5.00 and the threshold's COUNT would be increased by two. When the audit records are delivered to the clearinghouse, the threshold's COUNT would be reduced by two, and the threshold's LAST_ACKNOWLEDGMENT variable could be updated to reflect the date and time that the records were delivered. Similarly, when the \$5.00 is paid (e.g., when the audit records are acknowledged as having been processed by the clearinghouse), the threshold's VALUE would be reduced by \$5.00.

Table 1 provides an illustrative list of the types of thresholds used in one embodiment of the present invention, and the conditions under which the thresholds' state variables are updated.

0062914-03100

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8600

TABLE 1

Typ of Threshold	Stat Updat d
Acknowledgment Threshold	Updates its state when a group of audit records is successfully sent to the clearinghouse
Paid Threshold	Updates its state when a processed acknowledgment is received from the clearinghouse
Controlled Threshold	Updates its state in response to execution of a control program

As shown in Table 1, and as described in more detail below in connection with Fig. 7, in one embodiment acknowledgment thresholds and paid thresholds are updated in response to acknowledgments received from a clearinghouse. In contrast, in a preferred embodiment controlled thresholds are updated by special control programs. For example, a controlled threshold might be attached to a prepaid budget object, and the budget provider might use a special control program to manage the budget – e.g., to add additional funds to the prepaid budget in response to a consumer’s request. This mechanism thus gives the budget provider explicit control over when and how the controlled threshold, and hence the budget, is updated. Additional information on the generation and use of control programs such as the one referred to in this example can be found in commonly-assigned U.S. Patent Application No. _____, entitled “Systems and Methods for Controlling, Managing, Identifying, and/or Creating Objects in a Distributed Computing Environment,” filed July 31, 2000, which is hereby incorporated by reference in its entirety.

Referring once again to Fig. 4, in one embodiment triggers 401 each include a conditional expression 402 and an action 404. When the conditional expression is satisfied, the trigger fires and the action is carried out. Table 2 illustrates three types of conditions that can be evaluated in a conditional expression 402.

Types of Conditions

Types of Conditions	
VALUE	Evaluates the total monetary value of the audit records that reference this threshold.
COUNT	Evaluates the total count of audit records that reference this threshold.
ACKAGE	Evaluates how much time has elapsed since the last acknowledgment received from the clearinghouse.

```
value > 200USD
```

This conditional expression contains a target 602, an operator 604, and a limit 606. In this example, a VALUE is being evaluated, and the limit is a currency amount. If an ACKAGE were being evaluated, then the limit might be a time interval, and if a COUNT were being evaluated, the limit would be an integer.

As shown in Fig. 6B, the trigger expression may also contain logical operators 610. In addition, as shown in Fig. 6C, it is possible to have compound trigger conditions, where the trigger expression is represented as a list of lists, and where the contents of each row are logically ANDed, and the rows are logically ORed to form the boolean evaluation of the trigger expression. Referring to Fig. 6C, for example, list 620 specifies that if the consumer's system has not received an acknowledgment from the clearinghouse in the last 30 days, the consumer is allowed to accumulate \$500 in deferred payments. If the system has not received an acknowledgment in the last 60 days, the limit is \$100. And if the system has not received an acknowledgment in the last 90 days, then the limit is \$10.

As indicated previously, when a conditional expression associated with one of a threshold's triggers is satisfied, the threshold is operable to signal transaction processing

application 112 to perform a predefined action. An illustrative list of trigger actions is set forth in Table 3.

TABLE 3

Types of Actions	
NOTIFY	Notifies the local system application that the condition has been satisfied
DELIVER	Delivers audit records to the clearinghouse
FAIL	Causes the associated transaction to be aborted
FAIL & NOTIFY	Causes the associated transaction to be aborted and notifies the local system application

Thresholds are evaluated when transactions occur (such as the purchase of content) and when transaction acknowledgments from a clearinghouse are processed. When a threshold is evaluated, each of its triggers is evaluated. In one embodiment, a trigger fires, or invokes its action, when the trigger condition changes from FALSE to TRUE. Once a trigger fires, it becomes incapable of firing again (i.e., it is “disarmed”) until the condition is first changed from TRUE back to FALSE, at which point the trigger is “armed” again, and becomes ready to fire when the condition is satisfied.

TABLE 4

Event	Threshold Value	Result
Content purchase of \$5	\$95	Trigger does not fire (armed but condition is false).
Content purchase of \$6	\$101	Trigger fires (armed and condition is true).
Content purchase of \$7	\$108	Trigger does not fire (disarmed and condition is true).
Acknowledgment for \$10	\$98	Trigger does not fire (armed and condition is false).
Content purchase of \$3	\$101	Trigger fires (armed and condition is true).

The triggers of all of the thresholds associated with a transaction are preferably evaluated as a group in two passes. In the first pass, triggers containing the FAIL or FAIL & NOTIFY actions are evaluated. If any of these triggers fire, the transaction is aborted and no further threshold processing is performed. No values are updated, and it is as if the transaction never occurred. In the second pass, all other triggers are evaluated.

Referring once again to Fig. 4, a more-detailed example of the functionality and use of threshold 514 can now be provided. As shown in Fig. 4, type definition 412 indicates that threshold 514 is an acknowledgment threshold. Thus, as indicated in Table 1, threshold 514's state is updated when audit records are successfully sent to the appropriate clearinghouse. Threshold 514 might initially contain a COUNT of 0. Each time a transaction occurs, the COUNT of threshold 514 is incremented to reflect the number of records generated by the transaction, and the threshold's triggers are evaluated. If, for example, the consumer has accumulated 20 audit records, and attempts to perform a transaction that would result in the twenty-first audit record being stored, conditional expression 402a will evaluate to TRUE and trigger 401a will fire, causing DELIVER action 404a to be executed. The result is that the 20 accumulated audit records are delivered to the clearinghouse (or scheduled to be delivered). The

Thus, it can be seen that thresholds provide a mechanism by which vendors, clearinghouses, budget providers, and the like can limit their exposure to the loss of money, content, or transactional information due to malicious attacks or computer malfunctions. Moreover, by using interrelated thresholds or trigger conditions, relatively fine-grained protection can be obtained, since if one threshold or condition is rendered inoperative due to system failures or attacks, other thresholds or conditions may still be operable to govern subsequent transactions.

Although the foregoing invention has been described in some detail for purposes of clarity, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.